UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

NASIA SANCHEZ, individually and on behalf of all others similarly situated, Plaintiff, v. PANERA, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Nasia Sanchez ("Plaintiff" or "Plaintiff Sanchez"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members" as defined below) and by and through her undersigned counsel, files this Class Action Complaint against Defendant Panera, LLC ("Panera" or "Defendant") and alleges the following based upon personal knowledge of facts pertaining to herself and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused her and the other Class Members in the large and preventable data breach that was discovered by Panera on March 23, 2024, and announced publicly by Panera on June 13, 2024, in which unauthorized users accessed Panera servers that contained personal information of current and former employees and business partners ("Data Breach" or "Breach").[1]

[1] *See* https://oag.ca.gov/system/files/Panera_CA%20App%20%26%20Sample_0.pdf.

2. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, some businesses still fail to put adequate security measures in place to protect their customers' and employees' data.

3. Defendant Panera, an American chain store of bakery-café restaurants, is renowned for providing a diverse menu that includes pastries, coffee, pizzas, salads, pasta, and more. With sales amounting to $6.34 billion in 2022, Defendant is ranked as the second-largest bakery café chain in the United States.[2]

4. The Data Breach itself occurred on February 9, 2024, during which an unauthorized third party gained access to Defendant's internal files that contained sensitive employees' data.[3] However, it took Defendant until March 23, 2024, to finally discover it, over a month later.[4] Although Defendant has not yet disclosed the total number of individuals affected, its investigation confirmed on May 16, 2024, that those files compromised contain employees' Personally Identifiable Information ("PII"), including but not limited to, full names and Social Security numbers.[5] On or around June 13, 2024, Defendant began sending letters ("Notice Letters") to affected individuals notifying them that their information was compromised. According to the Notice Letter, other information that Defendant collected from affected individuals upon their employment might also have been impacted.[6] However, no additional details have been announced yet.

5. As a condition of employment, Plaintiff and the Class Members were required to disclose their PII to Defendant, entrusting Defendant with keeping it safe and protected.

---

[2] *See* https://www.statista.com/statistics/1115824/bakery-cafe-chains-highest-sales-us/(last visited June 18, 2024).
[3] Defendant's report to the Office of the Maine Attorney General: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/9366354d-de2c-468a-9e81-7fece7463aeb.html (last visited June 18, 2024).
[4] *See* https://oag.ca.gov/system/files/Panera_CA%20App%20%26%20Sample_0.pdf.
[5] *Id.*
[6] *Id.*

6. As a corporation doing business in Missouri, Defendant is legally required to protect the PII it gathers from unauthorized access and exfiltration. Given Defendant's sophistication as a well-known business, it knows and should have known its legal obligation to safeguard its cybersecurity.

7. The Data Breach was the result of Defendant's failure in establishing, implementing, and maintaining reasonable policies and adequate procedures to safeguard the PII it collected as part of its business. This unencrypted PII was compromised due to Defendant's negligent and/or careless actions and its complete failure to protect the PII of its users. Hackers targeted and acquired the PII of Plaintiff and Class Members because of its value in exploiting and stealing the identities of Plaintiff and Class Members.

8. Given the particularly sensitive nature of the exposed data, Plaintiff and Class Members have suffered irreparable harm and are subject to an increased risk of identity theft for the foreseeable future.

THE PARTIES

9. Defendant Panera is an American chain store of bakery-café restaurants headquartered in St. Louis, MO.

10. At all relevant times, Plaintiff Nasia Sanchez is an adult individual and a natural person of New Jersey, residing in Mercer County, where she intends to stay.

11. Plaintiff Sanchez, a former employee of Panera, provided her PII, including at least, her full name, address, bank account information, birth certificate, and Social Security number ("SSN"), to Panera as a condition of employment.

12. Plaintiff reasonably believed Defendant would keep her PII secure. Had Defendant disclosed to Plaintiff that her PII would not be kept secure and would be easily accessible to hackers and third parties, she would not have provided it to Defendant.

13. Plaintiff Sanchez received a notice letter from Defendant, dated June 13, 2024,

informing her of the Data Breach and that her name, SSN, and potentially other information provided by her were all compromised in the Data Breach.

JURISDICTION AND VENUE

14. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one Class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in Missouri, and has sufficient minimum contacts with Missouri.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District.

17. Application of Missouri law to this dispute is proper because Defendant's headquarters are in Missouri, the decisions or actions that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in Missouri, and the action and/or inaction at issue emanated from Missouri.

FACTUAL ALLEGATIONS

A. Defendant collects and stores thousands of current and former employees' PII and fails to provide adequate data security

18. Founded in 1987, Defendant Panera, LLC, is an American chain store of bakery-café restaurants headquartered in St. Louis, MO. With over 2,000 locations throughout the United States and Canada, Defendant has approximately 14,000 employees as of 2023.

19. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and

to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their sensitive PII.

20. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from disclosure to third parties. However, Defendant failed to fulfill this duty.

B. Panera's inadequate data security exposes its employees' sensitive PII

21. On or about February 9, 2024, unknown third-party cyber criminals gained access to Defendant's system that stores employees' data. PII including at least employees' names and SSNs have been accessed and acquired by the hackers.

22. Plaintiff received a letter from Panera dated June 13, 2024 ("Notice Letter"), notifying her that her PII, including at least her full name and SSN, may have been compromised. Specifically, the Notice Letter states the following:

> Panera, LLC ("Panera") is writing to notify you of a security incident that involved some of your information. We understand the importance of protecting the information we maintain, and this letter explains what happened, the measures we have taken, and steps you may consider taking.
>
> Panera detected and took measures to address the incident on March 23, 2024. A cybersecurity firm was engaged. A thorough investigation identified unauthorized access to internal files occurring that day. We also notified law enforcement. The files involved were reviewed, and on May 16, 2024, we determined that a file contained your name and Social Security number. Other information you provided in connection with your employment could have been in the files involved. As of the date of mailing of this letter, there is no indication that the information accessed has been made publicly available.

C. The PII is valuable.

23. An active, robust, and legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[7]

[7] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited June 18, 2024).

24. "Ransomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[8]

25. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[9]

26. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to encryption, which allows users and criminals to conceal identities and online activity.

27. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, the stolen information often ends up on the dark web because the malicious actors buy and sell the information for profit.[10]

28. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries

[8] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/(last visited June 18, 2024).

[9] *See Ransomware Guide*, Multi-State Information Sharing & Analysis Center (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf. (last visited June 18, 2024).

[10] *Shining a Light on the Dark Web with Identity Monitoring,* IDENTITYFORCE (updated Feb. 1, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 18, 2024).

all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[11]

29. The PII of consumers is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13]

30. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

---

[11] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR CLOUD SECURITY (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/(last visited June 18, 2024).

[12] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/(last visited June 18, 2024).

[13] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/(last visited June 18, 2024).

[14] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/pubs/EN-05-10064.pdf#:~:text=Identity%20theft%20is%20one%20of%20the%20fastest%20growing,to%20apply%20for%20more%20credit%20in%20your%20name (last visited June 18, 2024).

31. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

32. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

33. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than other types of data because the information compromised in this Data Breach is difficult, if not impossible, to change.

34. The PII compromised in the Data Breach also demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[16]

35. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

36. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime

---

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen- by-anthem-s-hackers-has-millions-worrying- about-identity-theft (last visited June 18, 2024).

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, REDSEAL, (Feb. 6, 2015), https://www.redseal.net/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers/(last visited June 18, 2024).

Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2023, resulting in more than $12.5 billion in losses to individuals and business victims, a twenty-two (22) percent increase in losses suffered compared to 2022.[17]

37. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

38. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

39. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[19]

40. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

---

[17] *See* Federal Bureau of Investigation Internet Crime Report 2023, INTERNET CRIME COMPLAINT CENTER, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text (last visited June 18, 2024).

[18] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 5, 2007), https://www.gao.gov/products/gao-07-737 (last visited June 18, 2024).

[19] *Id.*

D. Panera failed to comply with Federal Trade Commission requirements

41. The FTC has issued several guidance documents for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[20]

42. The FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[21]

43. The FTC guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

44. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

45. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

---

[20] *Start With Security: A Guide for Businesses (Lessons Learned from FTC Cases)*, FED. TRADE COMM'N ("FTC") (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 18, 2024)

[21] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 18, 2024).

[22] *Start With Security: A Guide for Businesses (Lessons Learned from FTC Cases)*, FED. TRADE COMM'N ("FTC") (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 18, 2024).

Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

46. Defendant Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

47. Plaintiff and Class Members gave their PII to Defendant with the reasonable expectation and understanding that Defendant would comply with its duty to keep such information confidential and secure from unauthorized access.

48. Defendant has been on notice for years that Plaintiff's and Class Members' PII was a target for bad actors because, among other motives, the high value of the PII created, collected, stored, and maintained by Defendant.

49. Despite such awareness, Defendant failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiff's and Class Members' PII from unauthorized access that Defendant should have anticipated and guarded against.

50. Defendant was fully aware of its obligation to protect the PII of its employees because of its collection, storage, and maintenance of PII. Defendant was also aware of the significant consequences that would ensue if it failed to do so because it collected, stored, and maintained sensitive private information from millions of individuals and knew that this information, if hacked, would result in injury to Plaintiff and Class Members.

51. Despite understanding the consequences of insufficient data security, Defendant failed to adequately protect Plaintiff's and Class Members' PII, permitting bad actors to access and misuse it.

E. Defendant failed to comply with industry standards.

52. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes

solutions to defend against those cyber-attacks.[23] All organizations collecting and handling PII, such as Defendant, are strongly encouraged to follow these controls.

53. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[24]

54. Cybersecurity experts normally have identified data management companies, like Defendant, as being particularly vulnerable to cyberattacks because of the value of the PII which they collect, use, and maintain.[25]

55. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[26]

56. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

F. The data breach caused harm and will result in additional fraud.

57. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of

[23] *Critical Security Controls*, CENTER FOR INTERNET SECURITY (May 2021), *available at* https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 18, 2024).
[24] *See CIS Benchmarks FAQ*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited June 18, 2024).
[25] *See* Joao-Pierre S. Ruth, *Security Questions to Ask After the Zeroed-In Breach*, INFORMATION WEEK (Dec. 5, 2023), https://www.informationweek.com/cyber-resilience/security-questions-to-ask-after-the-zeroedin-breach (commenting that the growing outsourcing of data analytics work to third-party service providers may offer to malicious cyber-attackers novel "targets of opportunity" – breach one data manager and gain access to data from a multitude of sources) (last visited June 18, 2024).
[26] *See Critical Security Controls*, CENTER FOR INTERNET SECURITY (May 2021), *available at* https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 18, 2024).

their Private Information for months without being able to take available precautions to prevent imminent harm.

58. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' data are severe.

59. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

60. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[28]

61. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

62. As demonstrated herein, these and other instances of fraudulent misuse of the compromised PII has already occurred and are likely to continue.

63. As a result of Defendan's delay between the Data Breach in February 2024 and the notice of the Data Breach sent to affected persons in June 2024, the risk of fraud for Plaintiff and Class Members increased exponentially.

64. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[29]

---

[27] 17 C.F.R § 248.201 (2013).
[28] *Id.*
[29] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited June 18, 2024).

65. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[30]

66. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

67. Thus, Plaintiff and Class Members now constant surveillance of their financial and personal records, monitoring, and loss of rights, for the foreseeable future.

G. Plaintiff and Class Members suffered damages.

68. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law, including but not limited to, Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

69. Had Defendant remedied the deficiencies in their information storage and security

[30] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) available at: https://bjs.ojp.gov/library/publications/victims-identity-theft-2014 (last visited June 18, 2024).
[31] GAO, *Report to Congressional Requesters*, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited June 18, 2024).

systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they would have prevented intrusion into its information storage and security systems.

70. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, inter alia, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

71. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their

time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

72. While Plaintiff's and Class Members' PII has been stolen, Defendant continues to hold Plaintiff's and Class Members' PII. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

H. Panera's delay in identifying and reporting the breach caused additional harm

73. While the initial Data Breach occurred on February 9, 2024, affected current and former employees were not notified of the Data Breach until June 13, 2024, or later and are unaware of how long their PII has been exposed to cyber criminals, thus depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

74. As a result of Panera's potential delay in detecting and notifying the affected individuals of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

PLAINTIFF'S EXPERIENCE

75. Plaintiff Nasia Sanchez is a resident of Hightstown, New Jersey.

76. Plaintiff Sanchez was employed by Defendant for only about a week in May 2022. As a condition of her employment, Plaintiff Sanchez was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and SSN.

77. Since ending her employment with Defendant in 2022, Plaintiff Sanchez has not been engaged in any other relationship with Defendant.

78. Plaintiff Sanchez values her privacy and makes every effort to keep her personal information private.

79. Plaintiff Sanchez only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

80. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Sanchez suffered injury from a loss of privacy.

81. Plaintiff Sanchez has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Sanchez entrusted to Defendant. This information has inherent value that Plaintiff Sanchez was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

82. After the Data Breach occurred, Plaintiff Sanchez has experienced a significant increase in spam calls and phishing emails.

83. The Data Breach has also caused Plaintiff Sanchez to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

84. As a result of the actual harm, Plaintiff has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts.

85. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Sanchez to spend significant time dealing with issues related to the Data Breach,

which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and signing up for credit monitoring service and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

86. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Sanchez to suffer stress, fear, and anxiety, including concerns about whether this Data Breach might impact her children.

87. Plaintiff Sanchez has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CHOICE OF LAW

88. Defendant is headquartered in Saint Louis, Missouri. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

89. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's Missouri headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in Missouri. Finally, Defendant's breach of its duty to employees—including Plaintiff and Class Members—emanated from Missouri.

90. It is appropriate to apply Missouri law to the claims against Defendant in this case due to Defendant's significant contacts with Missouri. Defendant is headquartered in Missouri; the relevant decisions, actions, and omissions were made in Missouri; and Defendant cannot claim to be surprised by the application of Missouri law to regulate its conduct emanating from Missouri.

91. To the extent Missouri law conflicts with the law of any other state that could apply

to Plaintiff's claims against Defendant, application of Missouri law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

CLASS ACTION ALLEGATIONS

92. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who are employees or former employees, or business partners, of Panera or any of its affiliates, parents, or subsidiaries, who had their PII compromised as a result of the Data Breach that was publicly announced on June 13, 2024.

93. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Panera; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and Members of the judge's staff.

94. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

95. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein,

b. Whether Defendant's inadequate data security measures were a cause of the data security breach,

c. Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII,

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff

and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII,

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the data security breach,

f. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class Members' PII in violation of Section 5 of the FTC Act,

g. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

h. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

96. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

97. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

98. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and

adequately protected by Plaintiff and her counsel.

99. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

100. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

101. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public PII as a condition of employment.

102. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business, which affects commerce.

103. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that the information would be safeguarded.

104. By assuming the responsibility to collect and store this data, Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing,

and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected.

105. Defendant owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of its current and former employees.

106. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

107. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

108. Defendant owed a duty of care to Plaintiff and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees and the critical importance of adequately securing such information.

109. Defendant's obligation to implement reasonable security measures also stems from the special relationship between Defendant and Plaintiff and Class Members. This relationship was established because Defendant was entrusted with the confidential PII of Plaintiff and Class Members as a necessary component of their employment.

110. Defendant also had a duty to exercise appropriate clearinghouse practices to

remove former employees' PII as it was no longer required to retain pursuant to the law and regulations.

111. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses in the United States.

112. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach but failed to do so. It took Defendant approximately a month to detect the breach, followed by an additional two months to conduct an investigation. Even after concluding the investigation, Defendant delayed further by taking an additional month to finally notify Plaintiff and Class Members.

113. Defendant had and continues to have duties to adequately disclose that Plaintiff's and Class Members' PII within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by unauthorized third parties.

114. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that Class Members could take appropriate steps to mitigate the potential for identity theft and other damages.

115. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and Class Members.

116. Plaintiff and Class Members were within the class of persons the provisions of the FTC Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statutes were intended to guard against.

117. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

118. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

119. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

120. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

121. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

122. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

123. It was foreseeable that Defendant's failure to adequately safeguard PII would result in one or more types of injuries to Plaintiff and Class Members.

124. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

125. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

126. Defendant's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

127. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

128. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff

and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

129. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII, and the harm, or risk of imminent harm, suffered by Plaintiff's and the Class. PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

130. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

131. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

133. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

134. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' PII in an unsafe and insecure manner.

135. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT AND
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff and the Class)

136. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

137. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment.

138. Plaintiff and Class Members entrusted their PII to Defendant. In doing so, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen, as well as an implied covenant by Defendant to protect Plaintiff' PII in its possession.

139. In entering into the implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices would comply with relevant laws and regulations and align with industry standards.

140. Implicit in the agreement between Plaintiff and Class Members and Defendant's

obligation to: (a) take reasonable steps to safeguard that PII; (b) prevent unauthorized disclosure of the PII; (c) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (d) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain PII only under conditions that kept such information secure and confidential.

141. The mutual understanding and intent of Plaintiff and Class Members, on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing. Defendant required Plaintiff and Class Members to provide their PII as a condition of employment. Plaintiff and Class Members accepted the offers for employment and provided their PII.

142. In accepting the PII, Defendant understood and agreed that they were required to reasonably safeguard and otherwise ensure protection of the PII from unauthorized access or disclosure.

143. Plaintiff and Class Member would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant that Defendant would keep their PII reasonably secure.

144. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor and ensure that the PII entrusted to it would remain protected by reasonable data security measures and remain confidential.

145. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant by providing their PII at Defendant's request.

146. Defendant breached the implied contracts made with Plaintiff and the Class by failing to safeguard and protect their PII, by failing to delete the PII of Plaintiff and the Class once the employment ended, and by failing to promptly provide accurate notice to them that their PII was compromised as a result of the Data Breach.

147. In addition, while Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

148. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII of former employees, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendant's security systems failed to meet applicable legal and industry standards.

149. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

150. As a direct and proximate result of Defendant's breach of these implied contracts and implied covenants, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of their bargain.

151. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

152. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to enhance its data security measures. Specifically, this includes: (i) strengthening its data monitoring procedures; (ii) undergoing annual audits of those systems and procedures; and (iii) providing or continuing to provide comprehensive credit monitoring services to all Class Members for their lifetimes.

COUNT III
BREACH OF CONFIDENCE

(On behalf of Plaintiff and the Class)

153. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

154. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

155. Plaintiff's and Class Members' PII constitutes confidential and unique information. Indeed, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim.

156. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to any unauthorized third parties.

157. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

158. Defendant voluntarily received, in confidence, Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

159. Due to Defendant's failure to protect Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

160. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff

and Class Members have suffered damages as alleged herein.

161. But for the disclosure of Plaintiff's and Class Members' PII, which is in violation of the parties' mutual understanding of confidence, Plaintiff's and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

162. The unauthorized disclosure of Plaintiff's and Class Members' PII constitutes a violation of Plaintiff's and Class Members' understanding that Defendant would safeguard and protect the confidential and unique PII.

163. The concrete injury and harm that Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's failure to ensure protection of the PII of Plaintiff and Class Members.

164. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the PII compromised as a direct and traceable result of the

Data Breach for the remainder of the lives of Plaintiff and Class Members.

COUNT IV
Invasion of Privacy
(On behalf of Plaintiff and the Class)

165. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

166. Missouri established the right to privacy in Article 1, Section 15 of the Missouri Constitution.

167. Under Missouri law, the right of privacy is invaded when there is "(1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public." *Sofka v. Thal*, 662 S.W.2d 502, 510 (Mo. banc 1983).

168. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

169. Defendant owed a duty to its employees, including Plaintiff and Class Members, to keep their PII confidential.

170. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the type of information that is the subject of this action, is highly offensive to a reasonable person.

171. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their employment with Defendant, but privately, with the intention that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class Members were reasonable in their belief that

such information would be kept private and would not be disclosed without their authorization.

172. The Data Breach constitutes an unreasonable intrusion upon Plaintiff's and Class Members' seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

173. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

174. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

175. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

176. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

177. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members. As such, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

178. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth

herein.

179. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing it with their valuable PII.

180. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

181. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

182. Defendant acquired the PII through improper record retention practices, as it failed to disclose the previously alleged inadequate data security measures.

183. If Plaintiff and Class Members had known Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendant.

184. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

185. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect the PII.

186. Plaintiff and Class Members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

187. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, Plaintiff and Class Members plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Class)

188. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

189. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

190. Defendant further breached its fiduciary duties owed to Plaintiff and Class Members as former employees by failing to remove and otherwise destroy Plaintiff's and Class Members' PII from Defendant's systems, as Defendant's employment relationship had ceased and Defendant no longer had any valid purpose for the maintenance and storage of that data.

191. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties

owed to Plaintiff and Class Members by failing to properly encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

192. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

193. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses. As such, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

COUNT VII
DECLARATORY AND

INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

194. Plaintiff restates and realleges paragraphs 1 through 99 above as if fully set forth herein.

195. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

196. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

197. Defendant owes a duty of care to Plaintiff and Class Members to adequately secure their PII.

198. Defendant still possesses PII regarding Plaintiff and Class Members.

199. Since the Data Breach, Defendant has announced minimal, if any, changes to its data security infrastructure, processes, or procedures aimed at addressing the vulnerabilities in its computer systems and security practices that allowed the breach to occur and to prevent future attacks.

200. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

201. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

202. There is no reason to believe that Defendant's security measures have improved

since the Data Breach to sufficiently meet its contractual obligations and legal duties.

203. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring,

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems,

e. Ordering that Defendant not transmit PII via unencrypted email,

f. Ordering that Defendant not store PII in email accounts,

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services,

h. Ordering that Defendant conduct regular computer system scanning and security checks,

i. Ordering that Defendant routinely and continually conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other Members of the Class, respectfully requests the Court order relief and enter judgment in their favor and against Defendant as follows:

A. For an Order certifying the Classes, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for

the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient

to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: June 18, 2024

Respectfully submitted,

Maureen M. Brady MO#57800
McSHANE & BRADY, LLC
4006 Central Street
Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
ATTORNEYS FOR PLAINTIFFS

/s/ Anderson M. Berry
M. Anderson Berry (*pro hac vice forthcoming*)
Gregory Haroutunian (*pro hac vice forthcoming*)
Michelle Zhu (*pro hac vice forthcoming*)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com
mzhu@justice4you.com

Attorneys for Plaintiff and the Proposed Class